

07-0320

A

The Law Offices of
STRAUB & POKOTYLO

Michael P. Straub
 mike@sp-ip.com

John C. Pokotylo
 john@sp-ip.com

1 Bethany Road
 Suite 56, Bldg. 4
 Hazlet, NJ 07730

Telephone: 732-335-1222
 Facsimile: 732-335-1228
 Internet Site: www.sp-ip.com

June 30, 2000

UTILITY PATENT APPLICATION TRANSMITTAL LETTER

Assistant Commissioner of Patents
 Box **Patent Application**
 Washington, D.C. 20231

Sir:

Enclosed herewith for filing is the following
utility patent application:

Attorney Docket No.: **MS-65/2(127316.1)**

Applicants: **Yacov YACOBI et al.**

Title: **"METHODS AND APPARATUS FOR PROTECTING SIGNALS
 TRANSMITTED BETWEEN A SOURCE AND DESTINATION
 DEVICE OVER MULTIPLE SIGNAL LINES"**

PATENT APPLICATION FILING FEE CALCULATION

	<u>No. Filed</u>	<u>Less</u>	<u>Rate/Claim</u>	<u>Fee</u>
Total				
Claims	<u>37</u>	-20	17 x \$18.00	\$ 306.00
Independent				
Claims	<u>7</u>	-3	4 x \$78.00	\$ 312.00
			Minimum Filing Fee	\$ 690.00
			Multiple Dependency Fee	
			(if applicable - \$260.00)	\$ 00.00
			50% Reduction for Small Entity	
			(Independent Inventor, Non-profit	
			Corporation, or Small Business	
			Concern) - appropriate	
			verified statement attached	\$- 00.00
			TOTAL FILING FEE	\$1,308.00
			ASSIGNMENT RECORDATION	\$ 40.00
			TOTAL FEES DUE	\$1,348.00

-1-

METHODS AND APPARATUS FOR PROTECTING SIGNALS
TRANSMITTED BETWEEN A SOURCE AND DESTINATION DEVICE
OVER MULTIPLE SIGNAL LINES

5

RELATED APPLICATIONS

This application claims the benefit of U. S
Provisional Application No. 60/160,603, filed October 20,
1999.

10

FIELD OF THE INVENTION

15

The present invention relates to methods and
apparatus for transmitting and storing information and,
more particularly, to methods and apparatus for
discouraging, and/or protecting against, the unauthorized
copying or use of the content of transmitted and/or
stored information, e.g., video and/or audio signals.

20

BACKGROUND OF THE INVENTION

25

Currently, video continues to grow in
importance. Video is now used for entertainment,
business and educational purposes.

30

Consumer electronics (CE) devices such as
digital video disks (DVDs), video cassette recorders,
televisions, etc. are frequently used to record and/or
playback video information. While many current CE video
devices are analog devices such as VHS VCRs, as the cost

5 Theft of copyrighted information, e.g.,
commercial videos, is a major problem. In order to
discourage the copying of, e.g., analog video cassettes,
many video distributors intentionally insert noise, as a
"copy protection" scheme, into a synchronization portion
10 of the recorded signal. While this noise normally does
not significantly effect the viewing of the original
cassette, copying of such cassettes using conventional
VCRs tends to produce a copy that contains an annoying
amount of flicker. The flicker results from inaccuracies
15 associated with the copying process through which the
noise included in the synchronization signal is much more
noticeable in the copy than in the recording being
copied.

25 While CE devices are tending towards all
digital embodiments, analog interfaces with computer
monitors are likely to be favored over digital interfaces
for quite some time. Generally, for a digital signal to
accurately represent an analog video signal, the sampling
30 rate of the digital signal must be at least twice the
highest frequency component of the analog signal being

5

10

25

30

slight frequency affects in synchronization signals. For this reason, conventional analog video copy protection techniques, such as that described above, are generally ineffective when applied to video signals supplied to analog multi-sync computer monitors.

In addition to DVDs, digital high definition televisions are likely to become common in the next few years as digital television broadcasts begin and the price of digital television sets decreases.

In order to reduce the risk of unauthorized copying of copyrighted works, several companies, including Hitachi, Ltd., Sony, Intel, and others have proposed an industry standard for digital consumer electronics devices which involves the use of authentication and key exchange procedures along with data encryption and the use of a digital communication bus which complies with IEEE standard 1394. The bus is sometimes referred to as "1394 Firewire". The proposed standard, hereinafter referred to as the "5C Standard", is discussed in the 5C Digital Transmission Content Protection White Paper White Paper, Revision 1.0, dated July 14, 1998.

The 5C standard includes several features. Four such features are:

(1) Copy control requests - A source device can request a destination device to honor copy control requests including copy-never, copy-free, and copy-once requests.

(2) Use of certificates - A destination device proves its trustworthiness to a source device by presenting a digital certificate, e.g., an authentication key, and using a corresponding private key for communications with the source device. The certificate is issued by a certifying authority that has examined the destination device to determine that it will honor the 5C Standard copy control requests.

(3) A key exchange protocol - The protocol is used by the source and destination devices once the destination device has proved that it is certified to establish a session key (content encryption key) used for encrypting copyrighted information to be exchanged.

(4) Transmission of copyrighted information in encrypted form - Information subject to copy restriction requests is transmitted in encrypted form using the session key.

In the proposed standard, a central authority is responsible for reviewing and certifying devices as complying with 5C Standard copy control requests.

FIG. 1 illustrates a conventional device 100 for implementing the 5C Standard. Device 100 includes authentication and key exchange subsystem 116, optional system renewal subsystem 114, content cipher subsystem 120, IEEE 1394 bus interface 118, storage device 112 for storing video data to be transmitted as well as received video data, and digital bus 122 which is 1394 compliant.

In this system, authentication messages, system renewal messages, authentication keys, exchange keys and session keys, in addition to encrypted data, are passed between the system 100 and other devices via the bus 122. Interface 118 is responsible for electrically interfacing between bus 122 and system elements, such as authentication and key exchange subsystem 116 and content cipher subsystem 120. The authentication and key exchange subsystem receives and exchanges, via bus 122, authentication and key information as well as system renewal messages. The content cipher subsystem is responsible for encrypting video information prior to transmission and decoding received encrypted information using content keys provided by authentication and key exchange system 116, to the cipher subsystem.

Storage 112 stores un-encrypted video data, copyright status and system renewal information. The system renewal and copyright status information is provided to authentication and key exchange subsystem 116. The video residing at the storage device 112 is supplied to, or received from, the content cipher subsystem which is responsible for encoding/decoding video information passed over bus 122.

In the conventional device, copy protection status information is included in an initial transmission of data between devices along with authentication information, e.g., authentication keys. Copy protection status information indicates that encrypted data can be copied freely, copied for one generation

(copy-one-generation), never copied (copy-never) or is subject to a no more copies constraint (no-more-copies). An authentication key is established during authentication, which occurs at the beginning of each exchange of encrypted information between source and destination devices. The authentication key is used to encrypt an exchange key. The exchange key is used to establish and manage security of copyrighted content streams. A content (session) key is exchanged between source and destination devices in conventional device 100. The content key is used to encrypt/decrypt the content being exchanged. Authentication and key exchange subsystem 116 provides the content key, associated with a particular communication, to content cipher subsystem 120 for use in encoding/decoding the content being transmitted or received.

The 5C Standard was designed primarily for digital CE devices. A housing of such devices can normally be sealed in such a manner as to make access to the inside of the device difficult -- particularly since consumers rarely need access to the insides of devices such as television sets and VCRs. Furthermore, an amount of control a consumer can have over the data processing performed by most CE devices can be limited to a set of preselected operations, e.g., play, reverse, stop, etc.

Computer owners are accustomed to having easy access to internal components of their systems for upgrading and component replacement purposes. Accordingly, in most cases it would be unacceptable to

seal computer housings in such a manner as to deny the owner easy access to internal components of his(her) computer system. In addition, one strength of a personal computer is that it can run arbitrary programs that can interact at a low-level with computer hardware and an operating system. Practically, this means that if unencrypted bits flow through a computer system, often a process can be crafted to steal, e.g., copy, them.

For this reason, computers generally raise more concerns with regard to potential pirating of copyrighted information than, e.g., televisions and other CE products. Because of the ease with which copyrighted data can be copied by computer systems, it is unlikely that computer systems, e.g., personal computers (PCs), are likely to be certified as devices which implement the 5C Standard copy control requests with sufficient certainty to support issuance to it of a 5C certificate. Without such a certificate, a device will be unable to interact and exchange copyrighted information subject to copy constraints with 5C Standard CE devices. The likely inability for a computer system, as a whole, to be certified as a 5C Standard compliant device poses the threat that, in the future, computer systems will be unable to interface with many CE devices.

Another threat to computer system and CE device interoperability has been created by the film industry. A least one major film studio has threatened to refuse licensing high-resolution video if such video will be transmitted on unencrypted analog interconnects.

If copyright owners maintain such a position, it would preclude computer devices from transmitting HDTV to monitors using unencrypted analog lines. The purpose of this 5C Standard is to secure upcoming high-resolution video formats by making it difficult for individuals to connect recorders into the analog stream between a video player and the monitor. A problem with this standard is that it will increase the costs of monitors and video cards.

Unfortunately, an inability to receive certification for a computer system as 5C compliant would prevent that system from displaying copy retrieved movies and other high definition video content where the video is transmitted to a monitor using conventional unencrypted analog monitor interconnects.

In view of the above discussed threats to computer system/CE device interoperability, a need now exists for methods and apparatus that would allow a computer system, or at least a portion of a computer system, to interface and exchange data with 5C Standard devices subject to copy restrictions. In addition, a need also exists for methods and apparatus of implementing some form of encryption or scrambling of video signals on analog interconnects to address concerns of copyright owners regarding unauthorized copying of analog signals. From a commercial standpoint, it is desirable that any new methods and apparatus be at least

5

10

15

20

25

30

signals. For example, the false signal can be created by switching between the actual R, G, B signals according to a deliberately chaotic rule. Alternatively, the false signal can be generated by combining high frequency information from at least one of the actual R, G, B signals with a modulated pedestal signal.

In accordance with the present invention, the R, G, B and UV video signals are encrypted by performing a matrix multiplication operation thereon. A set of matrix coefficients, which are a function of the output of a pseudo random number generator, are used by the matrix multiplier when performing the matrix multiplication operation. The matrix coefficients may correspond to a permutation matrix which results in the position of the input signals being swapped on the output lines of the matrix multiplier.

The display device includes a pseudo random number generator that is synchronized with the number generator of the display adapter. A matrix multiplication operation, which is the inverse of the one performed during encryption, is performed to decrypt the encrypted video signals. The false video signal is discarded while the decrypted R, G, and B video signals are supplied to a display.

To avoid the need for an additional line between the display adapter and the display device beyond those found in conventional display cables, e.g., VGA

In order to free the horizontal synchronization line for use in conveying the fourth encrypted video signal, the horizontal synchronization information is combined with one of the other signals communicated from the display adapter to the display device. For example, in one case the horizontal and vertical synchronization information are combined into a single composite signal, e.g., a composite sync pulse train. The composite signal is then transmitted to the display device over the vertical synchronization signal line freeing the horizontal synchronization signal line to carry the fourth encrypted video signal.

In another case, the horizontal synchronization information is combined with one or more of the video signals being transmitted to the display device. In this regard, the horizontal blanking period of the video signal can be used to deliver data, including horizontal sync information, to the display device. Bi-phase encoding may be used to modulate the horizontal synchronization information on one or more video signals. Because the video signals will be swapped during transmission as part of the encryption process, it can be useful to incorporate the horizontal synchronization information in the four video signals being transmitted to the display. This allows the horizontal synchronization information to be extracted by monitoring

any one of the four lines used to communicate video signals during encrypted mode operation.

5 In the case where horizontal sync information is incorporated into the video signals transmitted to a display device, a display adapter of the present invention initially provides unencrypted R, G, and B video signals including horizontal synchronization information to the display device. Horizontal and
10 vertical synchronization information are also provided, at least initially, over the horizontal and vertical synchronization lines, respectively.

15 Once certification and authentication of the display device has been accomplished via the exchange of signals over the plug and play line and/or the communication of data to the display over one of the other lines, the monitor switches to using the horizontal sync data received via the video signals, the computer
20 stops delivering conventional horizontal sync signals, and the display adapter begins to encrypt the video signals, e.g., by swapping the lines over which the R, G, B and addition false signal are transmitted.

25 The monitor reverts to conventional signaling, e.g., unencrypted mode operation, if it receives an explicit command to revert to unencrypted mode operation from the display adapter or if the horizontal sync data is lost for a period of time, e.g., two seconds. With
30 the ending of encrypted mode operation, the display adapter switches to providing unencrypted video signals

to the display device and to providing the horizontal synchronization signal in the normal manner over the horizontal synchronization line.

5 Through the above discussed methods, analog video signals can be encrypted, e.g., scrambled, in a relatively inexpensive manner which provides good protection from unauthorized descrambling and use of the encrypted video signals.

10

BRIEF DESCRIPTION OF THE DRAWINGS

15

Fig. 1 illustrates a block diagram of a conventional device capable of implementing the proposed SC standard for secure communication of information in consumer electronic devices;

20

Fig. 2 illustrates a computer system implemented in accordance with one embodiment of our present invention;

25

Fig. 3 illustrates a display adapter and display device coupled together in accordance with a first exemplary embodiment of the present invention;

Fig. 4 depicts a flow chart illustrating the operation of our inventive display adapter;

30

Fig. 5 illustrates our inventive display adapter of the present invention in greater detail;

Fig. 6 illustrates display device, as shown in FIG. 2, in greater detail; and

5 Fig. 7 illustrates a matrix multiplication operation that may be used to encrypt video signals in accordance with one exemplary embodiment of the present invention.

10 Fig. 8 illustrates a display adapter and display device coupled together in accordance with a second exemplary embodiment of the present invention;

15 Fig. 9 illustrates the display adapter of Fig. 8 in greater detail.

20 Fig. 10 illustrates a signal generator, which may be used in accordance with the present invention, to generate a dummy analog video signal.

Fig. 11 illustrates an exemplary modulated pedestal signal which may be generated by the modulated pedestal signal generator shown in Fig. 10.

25 Fig. 12 illustrates an exemplary dummy video signal which may be generated by the signal generator shown in Fig. 10.

30 Fig. 13 illustrates an exemplary display device suitable for use as the display device shown in Fig. 8.

5 Fig. 15 illustrates the display adapter of Fig.
14 in greater detail.

10

15

DETAILED DESCRIPTION

20

25

30

particular abstract data types. Moreover, those skilled in the art will appreciate that at least some aspects of the present invention may be practiced with other configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics; network computers, minicomputers, set-top boxes, mainframe computers, displays used in, e.g., consumer electronics applications, automotive, aeronautical, industrial applications, and the like. At least some aspects of the present invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices linked through a communications network. In a distributed computing environment, program modules may be located in local and/or remote memory storage devices. Nevertheless, to facilitate understanding, we will discuss our invention in the context of various embodiments that would be used in a PC environment.

FIG. 2 and the following discussion provide a brief, general description of an exemplary apparatus in which at least some aspects of the present invention may be implemented. Various methods of the present invention will be described in the general context of computer-executable instructions, e.g., program modules, being executed by a computer device such as computer system 220 or display adapter 248. Other aspects of the invention will be described in terms of physical hardware such as, e.g., display adapter circuits and display device components.

System 200 includes general purpose computing device 220 taking the form of, e.g., a PC. PC 200 may include processing unit 221, system memory 222 and system bus 223 that couples various system components including the system memory to processing unit 221. System bus 223 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures.

The system memory may include read only memory (ROM) 224 and/or random access memory (RAM) 225. Basic input/output system 226 (BIOS), including basic routines that transfer information between elements within PC 220, such as during start-up, may be stored in ROM 224.

PC 200 may also include hard disk drive 227 for reading from and writing to a hard disk (not shown), magnetic disk drive 228 for reading from or writing to (e.g., removable) magnetic disk 229 and optical disk drive 230 for reading from or writing to removable (magneto) optical disk 231, such as a compact disk or other (magneto) optical media. Hard disk drive 227, magnetic disk drive 228 and (magneto) optical disk drive 230 may be coupled with system bus 223 through hard disk drive interface 232, magnetic disk drive interface 233 and a (magneto) optical drive interface 234, respectively. The drives and their associated storage media provide nonvolatile storage of machine readable instructions, data structures, program modules and other data, e.g., video data. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk and a removable optical disk, those skilled in the art will

appreciate that other types of storage media, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read only memories (ROM), and the like may be
5 used instead of, or in addition to, the storage devices introduced above.

A number of program modules may be stored on hard disk 223, magnetic disk 229, (magneto) optical
10 disk 231, ROM 224 or RAM 225, such as, e.g., operating system 235, one or more application programs 236, other program modules 237 and/or program data 238. A user may enter commands and information into PC 220 through input devices, such as, e.g., keyboard 240 and pointing
15 device 242. Other input devices (not shown) such as a microphone, joystick, game pad, satellite dish, scanner, or the like may also be included. These and other input devices are often connected to the processing unit 221 through serial port interface 246 coupled to the system
20 bus. However, input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB) -- all of which are not shown.

A display device, e.g., monitor 247,
25 implemented in accordance with the present invention is connected to system bus 223 via an interface, such as inventive display adapter 248. In addition to being coupled to monitor 247 and system bus 223, display adapter 248 is coupled to external DVD player 251 via
30 IEEE 1394 standard digital data bus, e.g., 1394 Firewire 249. Video adapter 248 can receive encoded

video via bus 249 or unencoded video via, e.g., system
bus 248. Bus 249 connects video adapter 248 directly to
5C Standard compliant CE devices without having to pass
encrypted information from a CE device through other
5 computer system components.

As will be discussed below, monitor 247 is
capable of interacting and exchanging identification
certificates (authentication keys) and session keys, in
10 accordance with the present invention, with video
adapter 248.

In addition to monitor 247, PC 220 may include
other peripheral output devices (not shown), such as,
15 e.g., speakers and printers.

PC 220 may operate in a networked environment
which defines logical connections to one or more remote
computers, such as remote computer 259. Remote
20 computer 259 may be another PC, a server, a router, a
network computer, a peer device or other common network
node, and may include many or all of the elements
described above relative to PC 220, although only memory
storage device 250 has been illustrated in FIG. 2. The
25 logical connections depicted in this figure include local
area network (LAN) 251 and wide area network (WAN) 252,
which may comprise, e.g., an intranet and Internet,
respectively.

30 When used in a LAN, PC 220 may be connected to
LAN 251 through network interface card (adapter)

("NIC") 253. When used in a WAN, such as the Internet, PC 220 may include modem 254 or other means for establishing communications over the wide area network. The modem, which may be internal or external, may be
5 connected to system bus 223 via serial port interface 246. In a networked environment, at least some of the program modules depicted relative to PC 220 may be stored in the remote memory storage device. The network connections shown are exemplary and other means of
10 establishing a communications link between the computers may be used.

FIG. 3 illustrates display adapter 248 and display device 247, shown in FIG. 2, embodiment coupled together in accordance with the present invention. As
15 illustrated, video adapter 248 can receive input from either system bus 223 or 1394 Firewire 249. In addition, video adapter 248 can receive monitor identification and video decoding synchronization information from display
20 device 247 via one or more plug and play (PP) lines 312.

Video adapter 248 can supply video information to display device 247 over a plurality of analog lines, here color signal lines 302, 304, 306; vertical
25 synchronization (VS) signal line 308, and horizontal synchronization (HS) signal line 310. Lines 302, 304, 306, 308, 310, 312 are typically part of a single multi-wire cable having a conventional D end connection for plugging into a corresponding D connector included in
30 an I/O interface of video adapter 248. As the result of the use of a conventional connector and pin-out

arrangement, the video adapter can be connected to a conventional, e.g., VGA, monitor, or monitor 247 capable of supporting encryption.

5 FIG. 4 depicts flow chart 350 illustrating the operation of our inventive display adapter 248.

As shown, upon power up or re-initialization, operation of display adapter 248 begins in step 352
10 wherein the display adapter 248 polls any display device, coupled thereto, to request monitor identification information. The polling may be done by transmitting a request for monitor identification information to the device on any one of the lines 302, 304, 406, 308, 310 or
15 312 and then waiting for a response from the display device via one or both of PP lines 312.

Hence, after transmitting a request for identification information, display adapter 248 monitors,
20 in step 354, PP lines 312 for a response from the display device.

If a response to the request is not received in a preselected amount of time (a "timeout" interval),
25 e.g., 1 second, as determined by decision step 356, display adapter 248 assumes that it is connected to a conventional analog display device, e.g., VGA monitor. Operation then proceeds to step 362. Through step 362, display adapter 248 restricts video output via the those
30 analog lines (302, 304 and 306, as shown in FIG. 3) to video information which is not subject to a restriction

prohibiting transmission of that information over unencrypted analog lines. From step 362 shown in FIG. 4, operation proceeds to step 364 wherein the lines 302, 304, 306 are used as R, G, and B analog video lines respectively, with analog video information being transmitted over these three lines to display device coupled to display adapter 248.

Video output occurs in step 364 until the system is reset or power is turned off causing, in step 370, operation of the display adapter to stop.

If, in step 356, a response to the request for display device identification information is detected within the timeout interval, then operation proceeds to step 358 wherein the identification information is examined. The identification information may be the same as or similar to the type used in the 5C Standard and include a digital certificate used to confirm the identity of the display device.

If the examination reveals, as determined by decision step 360, that the display device coupled to adapter 248 is not an encryption capable device, operation proceeds, via step 360, to step 362.

However, if the examination in step 358 reveals that the display device is a line swapping capable device, operation proceeds, via step 360, to step 366. This latter step periodically exchanges session key and synchronization information with the display device.

This may involve, for example, the display adapter transmitting synchronization and session key information to display device 247 on one or all of the signals appearing on signal lines 302, 304, 306 during a vertical blanking period.

With the exchange of a session key, display adapter 248 is ready to produce encrypted analog video signals on signal lines 302, 304, 306 which connect display adapter 248 to display 247. These signals are produced and applied to display device 247 through step 368. The periodic exchange of session key and synchronization information, as well as the supply of encrypted video signals to display 247, which occur in steps 366 and 368, continues until operation of display adapter 248 or display device 247 halt in step 370, e.g., due to power being turned off or a re-set operation being performed.

FIG. 5 illustrates our inventive display adapter 248. Display adapter 248 may be implemented, e.g., as a separate plug-in card or incorporated directly into a motherboard of a computer system. As illustrated, the display adapter comprises input/output interface 402, video processor 404, video signal encryption circuit 406, I/O interface 412, memory 405, 1394 content cipher subsystem 414, authentication and key exchange system 416, pseudo-random number generator 410 and matrix inverter circuit 408 coupled together as shown. The display adapter may include optional system renewal

subsystem 114 (shown in FIG. 1) coupled to authentication and key exchange subsystem 416.

I/O interface 402, shown in FIG. 5, includes
5 system bus interface (SBI) 402A for interfacing between system bus 223 and display adapter components including video processor 404. In addition, I/O interface 402 includes IEEE 1394 interface 249 to facilitate
10 interaction via the 1394 Firewire 249 between 5C Standard compliant devices and various components of the display adapter, e.g., 1394 content cipher subsystem 414 and authentication and key exchange system 416.

1394 content cipher subsystem 414 may be the
15 same as, or similar to, that used in conventional known device 100 (as shown in FIG. 1). Content cipher subsystem 414, receives, from authentication and key exchange subsystem 416, the content (session) key to be used for encoding/decoding information being processed
20 during a communication session and/or information relating to the encryption algorithm to be used. The content cipher subsystem decodes encoded data received via 1394 Firewire 249. Subsystem 414 also encodes data subject to copyright restrictions in accordance with the
25 5C Standard prior to transmission of that data via 1394 Firewire 249.

I/O interface 402 serves to couple 1394 content cipher subsystem 414 to video processor 404 and system
30 bus 223. Decoded video output produced by content cipher subsystem 414, copy restrictions permitting, can be

transmitted over system bus 223 or processed by video processor 404. Video data processed by video processor 404 can be applied to a display via the digital matrix multiplier 406 and second I/O interface 412.

5

In accordance with our inventive teachings, encrypted data received via 1394 interface 402B can be stored and transmitted in encrypted form in a portion of PC 220 which is external to display adapter 248.

10

However, to do so, the session key associated with the encrypted data would be maintained within secure display adapter 248 in, e.g., non-volatile memory 405. In this manner, the video data, being in encrypted form outside adapter 248, is thus protected, from unauthorized copying or editing. Since the display adapter stores the session key, stored encrypted video information can be played back at some future time through this adapter without compromising data security. This allows encrypted video information subject to copy restrictions to be stored safely, e.g., on hard disk 227 and later accessed, decrypted and rendered through the same display adapter. Doing so may be useful for some business and home applications where there is likely to be a delay between when copy restricted video information is received and ultimately viewed.

15

20

25

Note that for processing traditional non-secure video received over the 1394 Firewire, PC 200 (see FIG. 2) may edit this video information, save to disk, etc. in unencrypted form. However, when operating in secure mode, e.g., when processing information subject to

30

copy restrictions, portions of PC 200, other than the display adapter, act as a pipe for the encrypted data and a repository for secure content.

5 Video processor 404, shown in FIG. 5, processes the received video signals, for performing various processing operations thereon, and controls operation of video signal encryption circuit 406. Possible signal processing operations include, e.g., decoding MPEG video data, editing data, and converting digital video data and/or images into analog red, green and blue video signals. Video processor 404 may be implemented as a digital signal processing circuit with digital-to-analog (D/A) converters for generating the analog output signals. In addition to generating the red (R), green (G), and blue (B) analog video signals, video processor 404 generates vertical synchronization signals, horizontal synchronization signals, and display information request signals, and also responds to information provided, via plug and play line 312, by the display device.

25 Video processor 404 is coupled to memory 405 wherein various control routines 407 are stored. The memory may also include image processing routines. The control routines control video processor operation and display interaction, e.g., in accordance with the steps 350 shown in FIG. 4.

30 In addition to storing control routines 407, memory 405 may store authentication keys

(certificates) 418, exchange keys 420 and content/session keys 422. The authentication keys are used for proving the identity of display adapter 248 to other devices. Exchange keys are used for encrypting messages sent to devices coupled to display adapter 248. Content/session encryption keys are used for encrypting signals transmitted by the display adapter to a device coupled thereto, e.g., a 5C Standard compliant device or display device 247 that implements our inventive analog signal encryption technique.

Video processor 404 generates unencrypted R, G, and B video signals and also controls video signal encryption circuit 406 via CTRL signal.

When operating with a conventional monitor, i.e., a monitor that does not support encryption of analog video signals, the video processor limits its analog video signal output to video signals which are not subject to an analog signal encryption requirement. In such a case, video processor 404 controls video signal encryption circuit 406, via the CTRL signal, to output the R, G and B video signals without making alterations thereto. In such a case, the R, G and B video signals are output as analog video signals R', G' and B', respectively. These signals are then output via I/O interface 412 via corresponding signal lines 302, 304 and 306. I/O interface 412 may include a standard monitor connection for connecting the display adapter to conventional display devices as well as to inventive

display device 247. In this manner, display adapter 248 can interact with conventional display devices.

5 When interacting with display device 247, video signal encryption circuit 406 is controlled by processor 404 so that the analog R, G and B video signals generated by the video processor are encrypted to generate video signals R', G' and B', respectively.

10 The encryption of the analog signals is performed as a function of a session key generated by authentication and key exchange system 416. The session key is used to drive pseudo-random number generator 410. The output of the pseudo-random number generator can be
15 used directly by video signal encryption circuit 406, e.g., in the case of self inverting matrices or, alternatively, it may first be processed by matrix inverter circuit 408. The matrix inverter circuit processes the output of the pseudo-random number
20 generator to ensure that the processing performed by video signal encryption circuit 406 will be the inverse of that performed by display device 247 when it receives the encrypted analog video signals.

25 In one relatively simple embodiment, the video signal encryption circuit swaps, as a function of the pseudo-random number generator output, the R, G, and B video signals to generate video signals R', G' and B'. Here, the signals on lines 430, specifically 430a, 430b
30 and 430c, represent signals generated by switching the input to each line so that at any given time it is

5

10

15

20

25

30

"transformed" first (R'), second (G'), and third (B') video signals can be expressed as follows:

$$R' = a_1R + b_1G + c_1B$$

$$G' = a_2R + b_2G + c_2B$$

$$B' = a_3R + b_3G + c_3B$$

where:

R, G and B are original color video signals;
R', G', and B' are transformed "encrypted"
first, second and third video signals; and
 a_n , b_n and c_n are coefficients generated using a
pseudo-random number generator, e.g.,
generator 410, driven by a session key.

Our inventive encryption and corresponding
decryption transformations may be implemented as matrix
multiplication operations where all or some of the matrix
coefficients are generated by, or are a function of, the
output of a pseudo-random number generator driven by a
session key.

Such video signal encryption and decryption may
be done using either digital or analog circuitry. For
example, it may be accomplished on display adapter 248
using digital circuitry implemented as part of a digital
signal processor which serves as video processing
circuit 404. In the display device, e.g., monitor, where
little or no DSP circuitry may be present, the decrypting
may be done using analog circuitry.

Use of matrix inverter 408 ensures that the encoding/decoding operations will be the inverse of one another. It may, in some cases be easier to implement matrix inverter 408 using digital signal processor circuitry rather than through analog circuitry. Accordingly, it may be desirable to incorporate matrix inverter 408 into the inventive display adapter which is more likely, than the display device, to include a digital signal processor having extra processing capacity. However, if desired, matrix inverter 408 could be included in display device 247 as opposed to display adapter 248.

In accordance with our inventive teachings, a session key is used to drive pseudo-random number generator 410. However, before a session key can be established, as discussed above with regard to FIG. 4, display adapter 248 first verifies that the receiving device is a trusted display, in contrast to a pirate video recorder, via the exchange of a certificate identifying the display device. This may be done by, e.g., transmitting information to the display device via one or more of video lines 302, 304, 306, vertical and horizontal sync lines 308, 310 and plug and play line 312. Information from the display device may be received by video processor 404 via plug and play line 312. During normal operation, session key and synchronization information may be transmitted to the display in the horizontal or vertical blanking portion of the video signals.

Verifying the identity of the receiving, e.g., display, device and establishing a session key to be used for encrypting information transmitted between display adapter 248 and our inventive display 247 is similar to the verification and session key establishment problems addressed by the 5C standard.

Advantageously, the same type of digital certificate and content key used by 5C Standard devices is used by our present invention. However, the communication between the display adapter and display is over one or more of lines 302, 304, 306, 308, 310, 312 and not 1394 Firewire. Thus, the analog encryption scheme of the present invention is well suited for use in 5C standard devices where the establishment and exchange of session keys as part of an analog encryption session may be implemented using much of the authentication and key exchange functionality provided for 5C Standard compliance, e.g., authentication and key exchange system 416. Accordingly, our inventive analog encryption scheme is well suited for use in conjunction with, or as an enhancement to, the 5C Standard. Authentication and key exchange system 416 is coupled to video processor 404 to facilitate use of system 416 in establishing and maintaining analog video encryption sessions.

As discussed above, a session key is used to drive pseudo-random number generator 410 which generates coefficient values used during encryption/decryption. A rate at which the session key is changed affects the

level of security provided. To increase the complexity of cryptanalysis required to break the encryption, as compared to embodiments which do not modify the session key during an established communication session, a new session key can be used for each scan line of an image being transmitted to the display. For enhanced security, the session key can be modified multiple times during a single scan line thereby varying the coefficients used to encode the video signals corresponding to a scan line.

As discussed above, to eliminate a need for an inversion circuit and/or matrix inversion operation, self-inverting matrices may be used. FIG. 7 illustrates a matrix multiplication operation that may be performed by the video signal encryption circuit to encrypt R, G and B video signals. Reference numeral 602 indicates a self-inverse matrix that can be used to encrypt R, G, and B signals.

From a security standpoint, the values of the matrix used for encryption/decryption should be such that the matrix remains non-singular.

For decoding to accurately occur, display adapter and display device 247 need to be synchronized such that the correct session key is used for decoding each line of both transmitted and received video images. Synchronization should occur promptly after loss of synchronization, e.g., due to loss of power or a noise signal. One approach to maintaining synchronization is

to periodically establish a new session key, e.g., every few seconds, e.g., 5 seconds.

5 In the event display device 247 loses power, this display device can signal the display adapter via one of plug and play lines 312 to establish a new session key.

10 Alternatively, the display device can actively monitor and detect loss of adapter/display synchronization. Specifically, the display adapter transmits a frame counter value to the display device during each vertical blanking period. The display device maintains its own count of received frames which it then
15 compares to a value provided by display adapter 248. If a mismatch between the frame count provided by the display adapter and that maintained in the display device is detected by the latter, the display device signals the display adapter 248 to initiate a re-synchronization
20 operation.

25 Having described our inventive video encryption method and the interaction of video adapter 248 and display device 247, we will now describe display device 247 in detail.

30 FIG. 6 illustrates an exemplary embodiment of display device 247. This device includes I/O interface 502, display control logic 504, video signal decryption circuit 506, display 523, pseudo-random number generator 510 and authentication and key exchange

5

10

15

20

30

with other device and proving authenticity of display
device 247. Certificates containing, e.g.,
authentication keys 518, are stored in a memory (also not
shown) which forms part of system 516. Keys 518, 520,
5 522 may be stored in non-volatile tamper-resistant
memory, e.g., an epoxy coated memory device, to prevent
unauthorized access to these keys.

The session key established by the
10 authentication and key exchange system serves as input to
pseudo-random number generator 510. The output of the
pseudo-random number generator is used by the video
signal decryption circuit 506 in performing a decryption
operation. The pseudo-random number generator output
15 represents matrix coefficients which are used as part of
a matrix multiplication operation performed by video
signal decryption circuit 506. Hence, a session key
drives the pseudo-random number generators, used for
encrypting and decrypting, in display adapter 248 and
20 display 247, respectively.

Video signal decryption circuit 506 performs,
as a function of the pseudo-random number generator
output, inverse processing to that performed by
25 encryption circuit 406 of display adapter 248. In this
manner, the signals R', B', G' received via lines 302,
304, 306 are converted back into the unencrypted R, G,
and B video signals. The unencrypted R, G and B signals
are supplied, along with the vertical and horizontal
30 synchronization signals, to display 523 which may be,

e.g., a cathode ray tube (CRT) or liquid crystal display (LCD).

5 As discussed above, in accordance with various
embodiments of the invention, analog R, G, B video
signals are processed, e.g., subjected to a matrix
multiplication operation, to form encrypted R', G', and
B' video signals. In this manner, the lines over which
10 the analog R, G, B signals are transmitted are varied,
e.g., swapped, as the matrix coefficients used to perform
the matrix multiplication operation are varied, e.g., as
the output of the pseudo random number generator 510
changes.

15 While the swapping of the lines used to
communicate the R, G, B analog video signals can make it
difficult for an unauthorized individual to decrypt these
signals, still greater security can be achieved by
20 introducing an additional signal path, e.g., a fourth
line, over which the R, G, B signals may be communicated
to a display device. In accordance with such an
embodiment, a switched pattern of analog video signals
comprising R, G, B and a false video signal called UV,
25 can be delivered over the four lines available for the
communication of analog video signals.

30 Figs. 8 through 17 relate to embodiments
wherein four analog video signal paths are provided for
communicating analog video signals between a display
adapter and a display device. Various components in

these figures operate in a manner which is the same as,
or similar to, components in the previously described
embodiments. Such components are identified using the
same reference numerals used in the earlier figures. For
the purposes of brevity, such signal components will not
be described again in detail.

Fig. 8 illustrates an embodiment where an
additional analog video signal path, line 301, is
provided between a video adapter 848 and display device
847. Thus, in addition to signal paths 302, 304, 306,
the R, G, B video signals may be communicated between the
video adapter and the display device 847, over signal
path 301. In addition to the signal paths used to
communicate the analog R, G, B signals, vertical
synchronization, horizontal synchronization and plug and
play lines 308, 310, 312 exist between the video adapter
848 and display device 847.

In the Fig. 8 embodiment, the particular three
lines, out of the four available signal lines, which are
used to transmit the R, G, B video signals at any given
time can be varied as a function of the output of a
pseudo random number generator in generally the same
manner as previously described in the three line
embodiment. However, in the 4 line embodiment a 4x4
permutation matrix as opposed to a 3x3 permutation matrix
is used for encryption purposes since the signal swapping
occurs over 4 lines as opposed to 3 lines.

In a four line video signal embodiment such as that shown in Fig. 8, a home recording system which captures analog video signals from only the three commonly used signal paths 302, 304, 306 would be missing one fourth of the analog image data and thus one fourth of the image "depth".

Elimination of one fourth the width of the image is a standard measure used in the traditionally recognized practice of unwanted film stock destruction. Accordingly, depriving unauthorized individuals from one fourth of the image depth is a desirable goal when encrypting analog video signals.

Fig. 9 illustrates the video display adapter 848 of Fig. 8 in greater detail. Note that much of the display adapter circuitry shown in Fig. 9 is similar to that of the previously described display adapter 248 shown in Fig. 5 which transmits analog video data over three lines. However, the display adapter 848 includes a dummy video signal generator, a UV signal generator, 901 not present in the Fig. 5 embodiment. The Fig. 9 embodiment also includes modifications designed to support four analog video signal lines as opposed to three video signal lines. For example, in Fig. 9, a video signal encryption circuit 906 having 4 inputs and 4 outputs is used in place of the three input and three output encryption circuit of Fig. 5. The video signal encryption circuit 906 performs a matrix multiplication operation on the four analog video signal inputs, e.g.,

the video signals UV, R, G, and B to produce the four encrypted video signal outputs UV', R', G', and B'.

5 A 4x4 matrix, e.g., a 4x4 permutation matrix, is used by the video signal encryption circuit 906 when performing the encryption operation. The matrix coefficients are supplied by matrix inverter 908 and pseudo random number generator 910. The matrix inverter and pseudo random number generator 910 operate in a
10 similar manner as to the like named circuits of Fig. 5 but they are designed to work with 4x4 matrix values as opposed to 3x3 matrix values. Thus, during each period in which a set of matrix coefficients are used, the matrix inverter 908 and pseudo random number generator
15 910 generate 16 values, e.g., corresponding to the 16 coefficients of a 4x4 matrix used by the video signal encryption circuit.

20 As in the case of the previously described embodiment, the pseudo random number generator 910, is driven by the output of the authentication and key exchange system 416.

25 In the Fig. 9 embodiment, an input/output (I/O) interface 912 having four analog video signal inputs and outputs, in addition to vertical synchronization signal, horizontal synchronization signal, and plug and play (PP) inputs and outputs couples the video signal encryption circuit 906 and video processor 404, to the corresponding
30 analog signal lines 902, 302, 304, 306, 308, 310, 312.

The false video signal UV can be generated in accordance with the present invention in any one of several ways. In one embodiment the analog signal UV is set to a signal value which will produce a blank gray field. In an alternative embodiment, the signal UV is set to values representing geometric patterns with high intensities. While both exemplary false signals will have annoying effects if used with the real signals to generate an image, the false signal may be detectable by comparing its signal values to the signals on the other analog signal lines. This is because the content of the signal UV is independent of the actual R, G, B signal values which tend to have some relationship to each other since they correspond to the same image.

To further strengthen the encryption signal from attack, the UV signal may be generated by switching among the valid R, G, B signals following a deliberately chaotic pattern. In one such embodiment, the false signal UV is generated by switching between the valid R, G, B signals once or twice during the transmission of each horizontal line of image data. The resulting false signal UV causes an image displayed using the signal to look bad while being difficult to electronically discriminate from the valid signals.

An even "uglier" false signal UV, which is difficult to detect, can be generated by combining the high frequency information, e.g., signal information above .75 MHz, from a valid R, G, or B signal with a

modulated pedestal signal. An obnoxious looking pedestal signal would be a "wobble" pattern varying between one half and four Hz. In such an embodiment, with each cycle of the pedestal signal, the false signal UV will normally pass through the range of average intensity values used by the valid R, G, B signals. This makes it difficult to distinguish the false signal UV from the valid R, G, B signals.

Fig. 10 illustrates an exemplary UV signal generator 901. In the Fig. 10 embodiment, the UV signal generator 901 includes a high pass filter 1002, a modulated pedestal signal generator 1004 and a signal summer 1006. The high pass filter 1002 receives as its input one of the valid R, G, or B video signals, e.g., the R signal. The high pass filter 1002 outputs a signal representing the high frequency signal component of the valid R signal component which is supplied to a first input of analog signal adder 1006. The modulated pedestal signal generator 1004 generates a modulated pedestal signal which is supplied to the second input of adder 1006. The adder 1006 combines the high frequency signal component of a valid analog video signal with the pedestal signal generated by the pedestal signal generator 1004 to generate the false signal UV.

Fig. 11 illustrates an exemplary pedestal signal 1100 which may be generated by the modulated pedestal signal generator 1004. Note that the pedestal signal includes steps of varying sizes which repeat at the end of the period 1102. While only 3 steps are shown

in Fig 11, a large number of steps, e.g., in excess of 1000, may occur during each period.

5 Fig. 12 illustrates an exemplary false signal UV generated by the UV signal generator 901. Note the signal 1200 includes the high frequency signal component of the R signal modulated on the pedestal signal illustrated in Fig. 12.

10 The encrypted analog video signals, including the false signal UV, are transmitted over the four wires 902, 302, 304, 306 to the display device 847 of the present invention.

15 Fig. 13 illustrates a display device 847 suitable for decrypting and displaying the encrypted analog video signals transmitted using four wires. Many of the components of the Fig. 13 display device are the same as those of the display device 247 illustrated in
20 Fig. 6. Such components are identified using the same reference numbers as in Fig. 6 and will not be discussed again in detail. The display device 847 differs from the display device 247 in that it includes an I/O interface 1302 which is capable of handling the additional analog
25 signal line 902. It also differs from the display device 247 in that the pseudo random number generator 1310 generates values representing the coefficients of a 4x4 matrix as opposed to a 3x3 matrix as in the case of display device 247.

15

20

30

the four wire video signal communication embodiment illustrated in Fig. 8.

5 The use of an additional video signal line, e.g., a fourth video signal line, will require the use of a cable between the display adapter and display device which is different than those currently in use, e.g., standard VGA cables, assuming that the other video adapter/display device interconnects remain unaltered.

10 From a backwards compatibility standpoint, it is desirable that in at least some embodiments, four lines be capable of being dedicated to the communication of analog video signals while still allowing traditional
15 VGA monitor cables to be used to connect the display adapter to the display device.

20 Traditional VGA monitor cables used to connect display adapters of existing computer systems to monitors include five high frequency shielded lines or cores plus a line for the plug-and-play signal path. Three of the shield lines are normally used for the analog R, G, B signals while the fourth and fifth shield lines are used for the vertical and horizontal synchronization signals,
25 respectively.

30 In accordance with one embodiment of the present invention, while operating in encrypted mode, one of the vertical and horizontal synchronization lines is freed for use as the fourth analog video signal line. While operating in unencrypted mode, the video signal

lines are used in a conventional manner. The freeing of a horizontal or vertical synchronization line is performed by combining the lines synchronization functions with one of the other signal lines.

5

In one embodiment of the present invention, the function performed by the horizontal and vertical sync signals are combined in the display adapter to form a composite sync pulse train which is then transmitted over a single one of the vertical and horizontal synchronization lines to the display device. The display device decodes the received sync pulse train into separate horizontal and vertical synchronization signals which are then used in the same manner as the conventional horizontal and vertical synchronization signals.

10

Accordingly, in such an embodiment, the separate line 902 for the signal UV' is eliminated and, during encrypted mode operation, one of the lines 308, 310 is used to communicate the fourth analog video signal UV' while the other one of the lines 308, 310 is used to convey the combined horizontal and vertical sync pulse train. During unencrypted mode, the horizontal and vertical signals are transmitted over lines 308, 310 in a conventional manner.

15

20

25

30

Fig. 14 illustrates another embodiment of the present invention wherein a video adapter 1448 is coupled to a display device 1447 via six signal lines 302, 304, 306, 308, 310, 312. Because six signal lines are used

for coupling the video adapter 1448 to the display device 1447, a conventional VGA monitor cable can be used for this purpose facilitating backwards compatibility with display devices which do not support encryption.

5

In the Fig. 14 embodiment, during encrypted mode operation, horizontal synchronization information is combined with one or more of the other video signals, e.g., the R, G, and/or B video signals, transmitted to the display device 1447. This frees the horizontal synchronization line 310 to be used, during encrypted mode operation, to transmit the encrypted fourth video signal UV'. During unencrypted mode operation, the horizontal synchronization signal is communicated over the line 310 in the normal fashion. To indicate that line 310 is used to communicate the encrypted signal UV' during encrypted mode operation and the horizontal synchronization signal HS during unencrypted mode operation, the label UV'/HS is used in Fig. 14 at both ends of line 310.

Fig. 15 illustrates the display adapter 1448, of Fig. 14, in greater detail. The display adapter 1448 includes many components, such as the interface 402, 1394 content cipher subsystem 414, memory 405, authentication and key exchange system 416 which are the same as, or similar to the like named and numbered elements previously discussed in regard to Fig. 5. For the purposes of brevity such components will not be discussed again.

30

5

10

20

30

Signal processing operations which may be performed by the video processor 1504 include, e.g., decoding MPEG video data, editing data, and converting digital video data and/or images into analog red, green and blue video signals. Video processor 1504 may be implemented as a digital signal processing circuit with digital-to-analog (D/A) converters for generating the analog output signals. In addition to generating the red (R), green (G), and blue (B) analog video signals, video processor 404 generates display information request signals, and also responds to information provided, via plug and play line 312, by the display device.

Video processor 1504 is coupled to memory 405 wherein various control routines previously discussed with regard to Fig. 5 are stored.

When operating with a conventional monitor, i.e., a monitor that does not support encryption of analog video signals, the video processor 1504 limits its analog video signal output to video signals which are not subject to an analog signal encryption requirement. In such a case, video processor 1504 controls video signal encryption circuit 1507, via the CTRL signal, to output the R, G and B video signals without making alterations thereto. In addition, during unencrypted mode operation, the processor 1504 controls the video signal encryption circuit 1507 to output the horizontal synchronization

signal HS, generated by the video processor, so that it is supplied to the display device on line 310.

In this manner, during unencrypted mode operation, the R, G, B video signals and vertical and horizontal synchronization signals are transmitted to the display device in a conventional manner allowing a conventional display device to receive and display video information from the display adapter 1448.

The video processor 1504 can detect via the plug and play line, when it is interacting with a display device of the present invention, e.g., display device 1447, as opposed to a conventional display device. When interacting with display device 1447 of the present invention, video signal encryption circuit 1507 is controlled by processor 404 so that video signal encryption will be performed on the analog R, G and B video signals generated by the video processor. In addition, the video processor 1504 enables the HS data signal generator 1506 and programmable mixer so that the horizontal synchronization information will be incorporated into each of the R, G, B video signals and the false video signal UV. By incorporating the horizontal synchronization information into the video signals, the horizontal synchronization line 310 can be used for transmitting the fourth encrypted video signal UV'.

The HS data signal generator is responsive to the control signal CTRL from the video processor 1504 and

receives as its input, the horizontal synchronization
signal HS generated by the video processor 1504.
Optionally, the HS data signal generator 1506 may also
receive key encryption information (KEI) to be
5 transmitted to the display device.

During encrypted mode operation, the HS data
signal generator 1506 is enabled by the video processor
1504. The HS data signal generator 1506 generates, from
10 the horizontal synchronization signal produced by the
video processor, a horizontal synchronization (HS) data
signal which can be mixed with the analog video signals
to form a video signal which includes horizontal
information. The generated HS data signal is supplied to
15 a corresponding data input of the programmable mixer
1502.

UV video signal generator 901 generates a false
video signal from the R video signal as previously
20 discussed. Alternatively, the false video signal UV can
be generated in any one of a number of different ways.

The programmable mixer 1502 receives as its
input, the R, G, B analog video signals and the false
25 video signal UV generated by UV signal generator 901.

During encrypted mode operation, the
programmable mixer 1502 modulates the received horizontal
synchronization data on each of the analog R, G, B and UV
30 video signals to produce modulated video signals R*, G*,
B*, UV*. The programmable mixer 1502 inserts into each

horizontal blanking period a burst of bi-phase encoded data obtained from the HS data signal generator 1506. The leading edge of a horizontal sync signal may be defined as the beginning of the first data byte following an encoded bi-phase sync word. For any given mode with N cycles of sync word, it is desirable that horizontal sync pulse validity be gated by a count of N sync word cycles.

Thus, in the Fig. 15 embodiment each of the modulated video signals include the same horizontal synchronization information. Optionally, key encryption information included in the HS data may also be modulated on the video signals.

The modulated video signals R^* , G^* B^* and UV^* are supplied to the video signal encryption circuit 1507 and the matrix multiplier 1506 included therein. The matrix multiplier 1506 also receives as an input a 4×4 set of matrix coefficients, e.g., 16 matrix coefficients.

In one relatively simple embodiment, the matrix multiplier 1506 swaps, as a function of the pseudo-random number generator output, the R, G, and B and UV video signals to generate video signals R' , G' B' and UV' encrypted video signals. The signal swapping is performed through implementation of the matrix multiplication operation and the use of matrix coefficients which correspond to a permutation matrix. In such an embodiment, the signals on lines 1530a, 1530b, 1530c, and 1530d, represent signals generated by switching the input to each line so that at any given

time it is difficult to determine which of these four lines is being used to transmit the modulated R*, G*, B* and UV* video signals.

5 In one such embodiment, the lines used to communicate the R*, G*, B* and UV* signals between the display adapter and monitor are pseudo-randomly swapped on an image line by image line basis for the signals R', G', B' UV'. As in the case of the Fig. 5 embodiment, a session key, exchanged with the display device is used to drive the pseudo-random number generator, e.g., number generator 1510. Since the session key and pseudo-random number generation techniques are common to both the display adapter and display device, the display device can perform the inverse swapping operation to properly reconstruct the R, G and B video signals.

20 The matrix coefficients supplied to the matrix multiplier 1506 are generated as a function of a value produced by the authentication and key exchange system. In the illustrated embodiment, the authentication and key exchange system 416 controls the pseudo random number generator to periodically generate a set of matrix coefficients. The coefficients, in the case of self inverting matrix coefficients, are supplied directly to the matrix multiplier 1506. In the illustrated embodiment, the output of the pseudo random generator 1510 is not limited to being self inverting matrix coefficients. Accordingly, before being supplied to the matrix multiplier 1508, each generated set of, e.g., 16, matrix coefficients are subjected to a matrix inversion

process performed by the matrix inverter 1508. By performing the matrix inversion operation in the display adapter 1448, the need to perform an inversion operation in the display device is avoided.

5

The matrix multiplier 1507 performs a matrix multiplication operation on the modulated analog video signals input thereto to produce four encrypted analog video signals R', G' B' and UV'. The multiplication operation may be implemented using analog signal multipliers and adders. The R', G' and B' encrypted video signals are supplied, via I/O interface 1512 to the corresponding lines 302, 304, 306.

10

15

The fourth encrypted video signal UV', generated by the matrix multiplier 1506, is supplied to a first input of MUX 1509. The second input of the MUX 1509 is supplied with the horizontal synchronization signal HS generated by the video processor 1504.

20

25

30

During encrypted mode operation, the MUX 1509 is controlled by the control signal CTRL to output the encrypted fourth video signal UV'. During unencrypted mode operation the MUX 1509 is controlled by the control signal CTRL to output the horizontal sync signal HS generated by the video processor 1504. I/O interface 1512 couples the output of MUX 1509 to the line 310 used by conventional display devices for communicating the horizontal sync signal. Thus, during unencrypted mode operation the horizontal sync signal is output in a conventional manner while during encrypted mode, the

5

10

15

20

25

30

I/O interface 1702 is coupled to lines 302, 204, 306, 310, 308 and 312. Thus, the I/O interface 1702 receives the analog video signals R', G', B', either the fourth encrypted analog video signal UV' or the
5 horizontal synchronization signal HS, the vertical synchronization signal VS, and the plug-play signal PP.

The I/O interface 1702 links the plug and play line 312 to the display control logic and the
10 authentication and key exchange system 518. The plug and play line 312 is a bi-directional communication line. Thus, the display control logic 1704 and authentication and key exchange system 516 can exchange information, e.g., display type information, timing information and
15 other information, e.g., relating to the mode of operation to be used at any given time, with the display adapter 1448 over the line 312.

The vertical synchronization line 308 is
20 coupled by the I/O interface 1702 to the display 523 and to the authentication and key exchange system 518. Accordingly, the video adapter 1448 can transmit vertical synchronization information and/or additional information to the display 523 and to the authentication and key
25 exchange system 516 via vertical synchronization line 308.

The UV'/HS signal line 310 is coupled by the I/O interface 1702 to the display control logic 1704,
30 authentication and key exchange system 516, and to the decryption circuit 1707. Thus, the display control logic

1704 receives, along with the encrypted analog video signal UV', the timing and other information included in the video signal during encrypted mode operation.

5 The first, second and third analog encrypted video signals R', G', B' are supplied via I/O interface 1702 to corresponding inputs of the decryption circuit 1707. Thus, the decryption circuit 1707 receives as its inputs the four encrypted video signals R', G', B' and
10 UV'.

 In addition to receiving the four encrypted analog video signals, the decryption circuit receives a control signal from the display control logic used to
15 control whether the display device operates in an unencrypted mode or encrypted mode of operation.

 The display control logic includes a mode control circuit which is responsive to signals received
20 via the PP line 302 to place the display device in either an encrypted or unencrypted mode of operation. A mode control signal CTRL generated by the mode control circuit 1715 is used to control the operation of decryption device 1707. The mode control circuit 1707 also includes
25 an optional connection to one of the encrypted video signal lines, e.g., line 310. Accordingly, the mode control circuit can monitor the video signal line 310 for the presence of modulated horizontal synchronization information and initiate encrypted mode operation when
30 the sync signal is present and de-activate encrypted mode

operation when the horizontal sync signal in the encrypted video signal is lost or not detected.

In addition to the mode control circuit 1715,
5 the display control logic 1704 includes a data demodulator 1707 and a timing recovery circuit 1717. The data demodulator 1707 recovers data, e.g., encryption key and encryption synchronization information, that is modulated on the encrypted video signals in some
10 embodiments. The data recovered by the data demodulator 1707, when present, is supplied to the authentication and key exchange system 516.

The timing recovery circuit 1717 is used to
15 recover the horizontal synchronization information from the encrypted video signal UV' during encrypted mode operation. A demodulated horizontal synchronization signal (D-HS) generated by the timing recovery circuit 1717 is supplied to the video decryption circuit 1707.
20 The timing recovery circuit 1717 may perform DC restoration on the received video signal prior to extracting the horizontal sync data. A zero crossing detector incorporating hysteresis may also be used in implementing the timing recovery circuit 1717.
25 Horizontal sync timing recovery may be further strengthened by integrating several valid horizontal sync pulses into the video signal over a time window and by using other well known techniques.

30 The video signal decryption circuit 1707 includes a matrix multiplier 1706 and a MUX 1708 both of

which are responsive to the mode control signal generated by the display control logic 1704. The matrix multiplier includes R', G' B' and UV'/HS signal inputs.

5 During unencrypted mode operation, the received signals supplied to the R', G', B' video signal inputs of the matrix multiplier will be the unencrypted analog R, G, and B video signals respectively. Accordingly, during unencrypted mode operation, the matrix multiplier simply
10 passes these signals to its R, G, B signal outputs and thus the corresponding signal inputs of the display 523.

 The matrix multiplier 1707 receives the conventional horizontal synchronization signal HS at its
15 UV'/HS signal input during unencrypted mode operation. The received HS signal is supplied to a first data signal input of the MUX 1708. A second data signal input of the MUX 708 is coupled to the D-HS signal output of the display control logic 1704. The output of the MUX 1708
20 is coupled to the horizontal synchronization signal input of display 523. When the CTRL signal supplied by the model control circuit 1715 to the MUX 1708 indicates unencrypted mode operation, the MUX's first input is coupled to its output. However, during encrypted mode
25 operation, the MUX's second input is coupled to its output. Thus, during unencrypted mode operation the display device 523 is supplied by MUX 1708 with the signal HS received via the UV'/HS line 310. During encrypted mode operation the display 523 will be supplied
30 with the demodulated horizontal synchronization signal, D-HS, generated by the timing recovery circuit 1717.

During encrypted mode operation, the pseudo random number generator 1710 generates a 4x4 set of matrix coefficients as a function of a value supplied by the authentication and key exchange system. The generation of the set of matrix coefficients is synchronized by the authentication and key exchange system 516 so that the same matrix coefficients generated by the display adapter's pseudo random number generator at encoding time will be produced for decoding the received encrypted video signals. The matrix coefficients produced by the pseudo random number generator 1710 are supplied to a coefficient input of matrix multiplier 1706.

During encrypted mode operation, the matrix multiplier performs a matrix multiplication operation on the received R' , G' B' and UV' signals which is the inverse of that performed at encoding time. The resulting UV^* signal is discarded while the signals R^* , G^* , B^* are supplied to the corresponding red, green and blue signal inputs of display 523. Because of the way in which the horizontal synchronization information was modulated by the display adapter, the presence of the horizontal sync signal information does not interfere with the display of the image by the display device 523, i.e., the horizontal synchronization information will be eliminated as part of an ordinary signal clamping operation performed by the display 523.

5

10

What is claimed is:

1. A method of processing first, second, and third signals for use in a system having first, second, third and fourth signal lines, comprising:

generating a fourth signal;

generating, using a pseudo-random number generator, pseudo-random output values; and

changing, as a function of at least one of said pseudo-random output values, which ones of the first, second, third and fourth signal lines are used to transmit the first, second, third, and fourth signals.

2. The method of claim 1, wherein generating a fourth signal includes:

processing at least one of the first, second or third signals to generate the fourth signal from said at least one of the first, second, or third signals.

3. The method of claim 1, wherein generating a fourth signal includes performing the act of:

switching between at least two of said first and second signals to generate said fourth signal.

4. The method of claim 1, wherein generating a fourth signal includes:

performing a high pass filtering operation on one of said first, second and third signals to produce a filtered signal; and

combining the filtered signal with a modulated pedestal signal to generate said fourth signal.

1 6. The method of claim 5,
2 wherein the first, second, and third signal lines
3 couple a source device to a destination device, said
4 pseudo-random number generator contained within the
5 source device, the method further comprising:

1 7. The method of claim 6, wherein the first, second and
2 third signals are red, green and blue video signals,
3 respectively, the method further comprising the steps of:
4 encrypting horizontal synchronization
5 information into at least one of said red, green and blue
6 video signals prior to changing which ones of the first,
7 second, third and fourth signal lines are used to
8 transmit said first, second and third signals.

1 8. The method of claim 7, further comprising:
2 transmitting a horizontal synchronization
3 signal over said fourth line prior to using the fourth

4 line to transmit one of said first, second and third
5 video signals.

1 9. A method of processing first, second, and third
2 video signals, the method comprising:
3 generating a fourth video signal,
4 transmitting the first, second, third, and
5 fourth video signals over first, second, third and fourth
6 lines, the transmitting including:
7 periodically swapping the lines used to
8 transmit the first, second, third and fourth video
9 signals.

1 10. The method of 9, further comprising:
2 modifying at least one of said first, second
3 and third signals prior to transmitting them.

1 11. The method of claim 10, wherein modifying at least
2 one of said first, second and third signals includes:
3 modulating horizontal synchronization
4 information on each of said first, second, and third
5 video signals.

1 12. The method of claim 11, wherein periodically
2 swapping the lines used to transmit the first, second,
3 third and fourth video signals includes the act of:
4 performing a matrix multiplication operation on
5 the first, second, third and fourth video signals to
6 determine the line on which each of the video signals are
7 transmitted.

1 16. The method of claim 15, further comprising:
2 generating the fourth video signal from at
3 least one of the red, green and blue video signals.

1 20. The method of claim 15, wherein combining the
2 horizontal synchronization information with at least one
3 of the vertical synchronization signal, red video signal,
4 green video signal and blue video signal includes:
5 combining the horizontal synchronization
6 information with the vertical synchronization signal to
7 form a composite synchronization signal including
8 horizontal and vertical synchronization information.

1 22. The method of claim 21, further comprising:
2 performing a demodulation operation on at least
3 one of the first, second, third and fourth video signals
4 to recover horizontal timing information.

1 24. The method of claim 22, further comprising:
2 exchanging a session key with a display
3 adapter; and
4 using the session key to control the pseudo
5 random number generator.

1 25. The method of claim 21, wherein performing a
2 decryption operation includes:
3 performing a matrix multiplication operation,
4 on the received first, second, third, and fourth video

5 signals, as a function of at least one value generated by
6 the pseudo random number generator, to produce said red,
7 green and blue video signals.

1 26. A method of operating a display device, the display
2 device including first through fifth inputs, the method
3 comprising:

4 during a first period of time,
5 receiving red, green and blue video signals on
6 the first, second and third inputs;
7 receiving a horizontal synchronization signal
8 on a fourth input;

9 receiving a vertical synchronization signal on
10 a fifth input; and

11 during a second period of time,
12 receiving first, second, and third encrypted
13 video signals on the first, second, and third inputs;
14 receiving a fourth encrypted video signal on a
15 first one of the fourth and fifth lines; and
16 receiving a vertical synchronization signal on
17 a second one of the fourth and fifth lines.

1 27. The method of claim 26, further comprising, during
2 the second time period of operation:

3 demodulating a horizontal synchronization
4 signal included in at least one of the first, second,
5 third and fourth encrypted video signals.

1 28. The method of claim 27, further comprising, during
2 the second time period of operation:

3 performing a decryption operation on the first,
4 second, third and fourth encrypted video signals to
5 generate red, green and blue video signals; and
6 generating an image on a display from said
7 generated red, green and blue video signals.

1 29. A video adapter comprising:

2 a pseudo random number generator;

3 a video signal generator for generating a
4 fourth video signal;

5 means for performing, as a function of a value
6 generated by said pseudo random number generator, a video
7 signal encryption operation on first, second, and third
8 video signals and said fourth video signal to produce
9 first, second, third, and fourth encrypted video signals.

1 30. The video adapter of claim 29, wherein the video
2 signal generator includes means for generating said
3 fourth video signal from at least one of said first,
4 second and third video signals.

1 31. The video adapter of claim 30, wherein the means for
2 performing a video signal encryption operation includes a
3 matrix multiplier.

1 32. The video adapter of claim 29, further comprising:

2 means for modulating horizontal synchronization
3 information on one of the first, second, third, and
4 fourth video signals.

1 33. The video adapter of claim 29,

0060877-063000

2 wherein the first, second, third and fourth
3 video signal are analog video signals; and
4 wherein the first, second, third and fourth
5 encrypted video signals are analog signals.

1 34. A display device, comprising:
2 a pseudo random number generator;
3 a video decryption circuit for performing, in
4 parallel, a video decryption operation on first, second,
5 third and fourth encrypted video signals as a function of
6 at least one value output by said pseudo random number
7 generator to produce analog red, green and blue video
8 signals.

1 35. The display device of claim 34, wherein the video
2 decryption circuit includes means for performing a matrix
3 multiplication operation on the first, second, third and
4 fourth encrypted video signals.

1 36. The display device of claim 35, further comprising:
2 means for demodulating horizontal
3 synchronization information included in at least one of
4 the first, second, third and fourth encrypted video
5 signals.

1 37. The display device of claim 36, further comprising:
2 means for supplying a horizontal signal
3 generated by said means for demodulating to a display
4 during an encrypted mode of display operation; and

5
6
7
1

ABSTRACT OF THE DISCLOSURE

Methods and apparatus for protecting copyrighted information, e.g., video signals, from unauthorized use are described. Encrypted video signals are transmitted from a source device, e.g., display adapter, to a display device, e.g., monitor, over analog signal lines after the identity of the destination device is confirmed by receipt of a certificate assigned to the destination device. A session key, used for encrypting the analog signals, is generated and exchanged between the source and destination devices. The source and destination devices each include a pseudo-random number generator driven by the session key. As part of the encryption process a false video signal is generated. The false video signal and R, G, B video signals are transmitted to the display device over four lines. The lines used to transmit the R, G, B and false video signals are periodically swapped as a function of the output of the pseudo random number generator to encrypt, e.g., scramble, the video signals. To avoid having to provide an additional line between the display adapter and the display device beyond those used in conventional displays, horizontal synchronization information is combined with, e.g., modulated on, one or more of the other signals transmitted to the display. The horizontal sync line is then used to convey one of the four video signals. The display device extracts the horizontal timing information from the received video signals and decrypts the signals using the output of its pseudo random number generator to reverse the scrambling process used to encrypt the transmitted video signals.

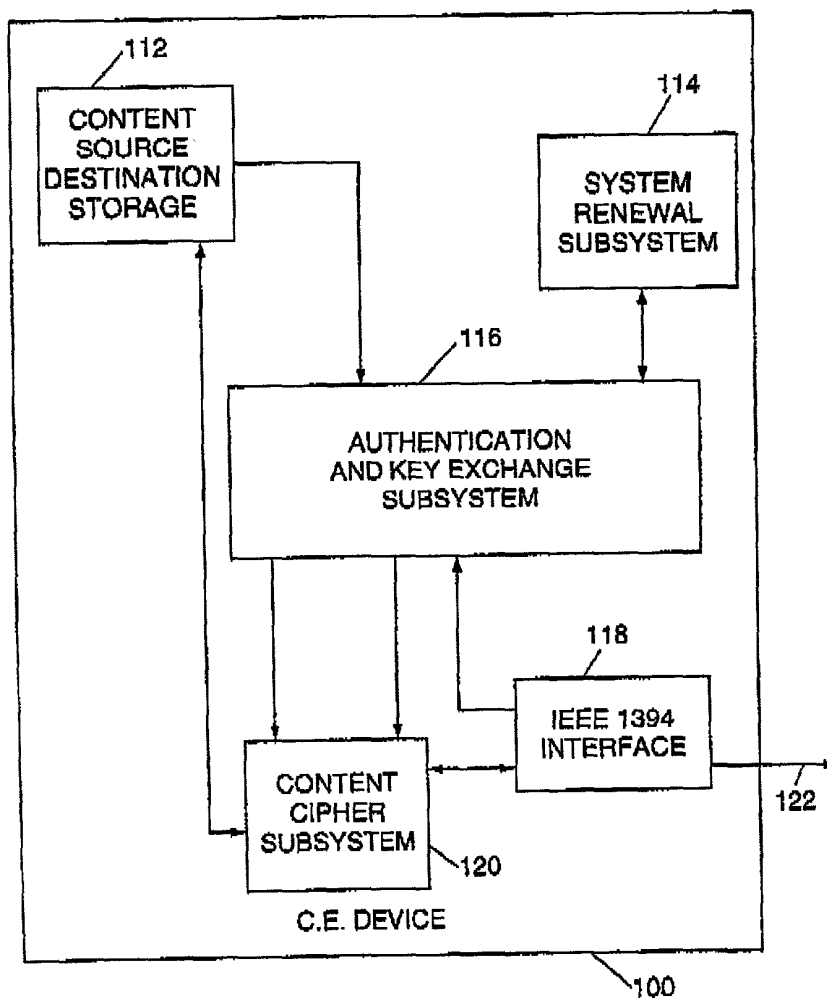


FIG. 1

PRIOR ART

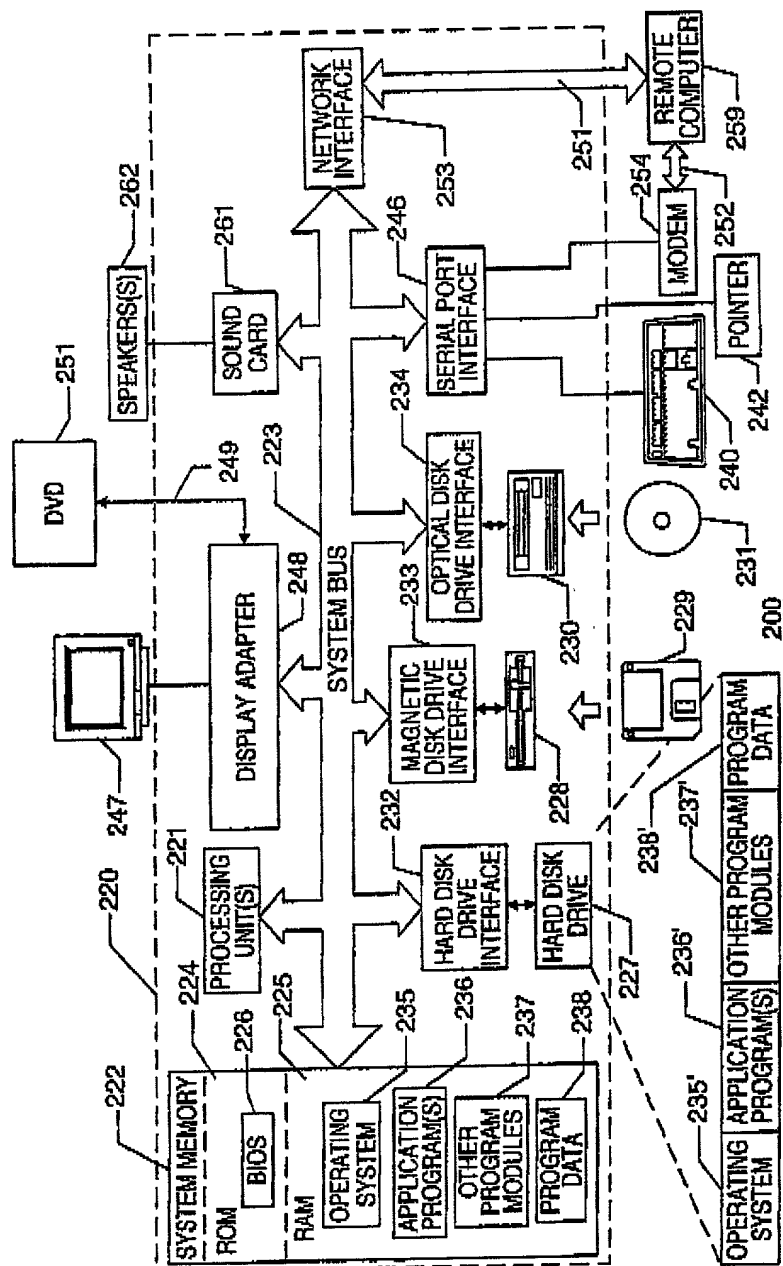


FIG. 2

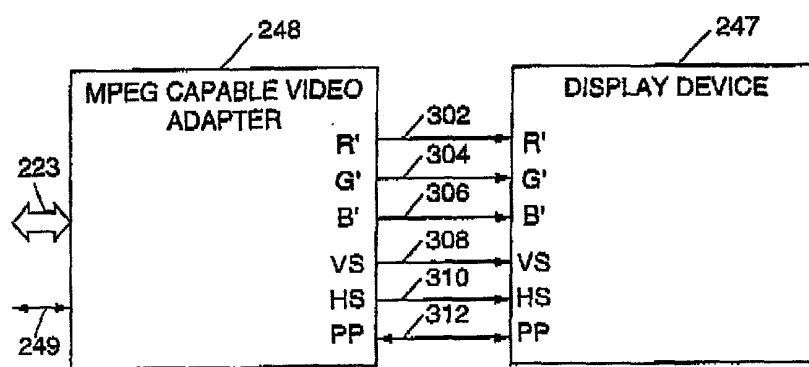


FIG. 3

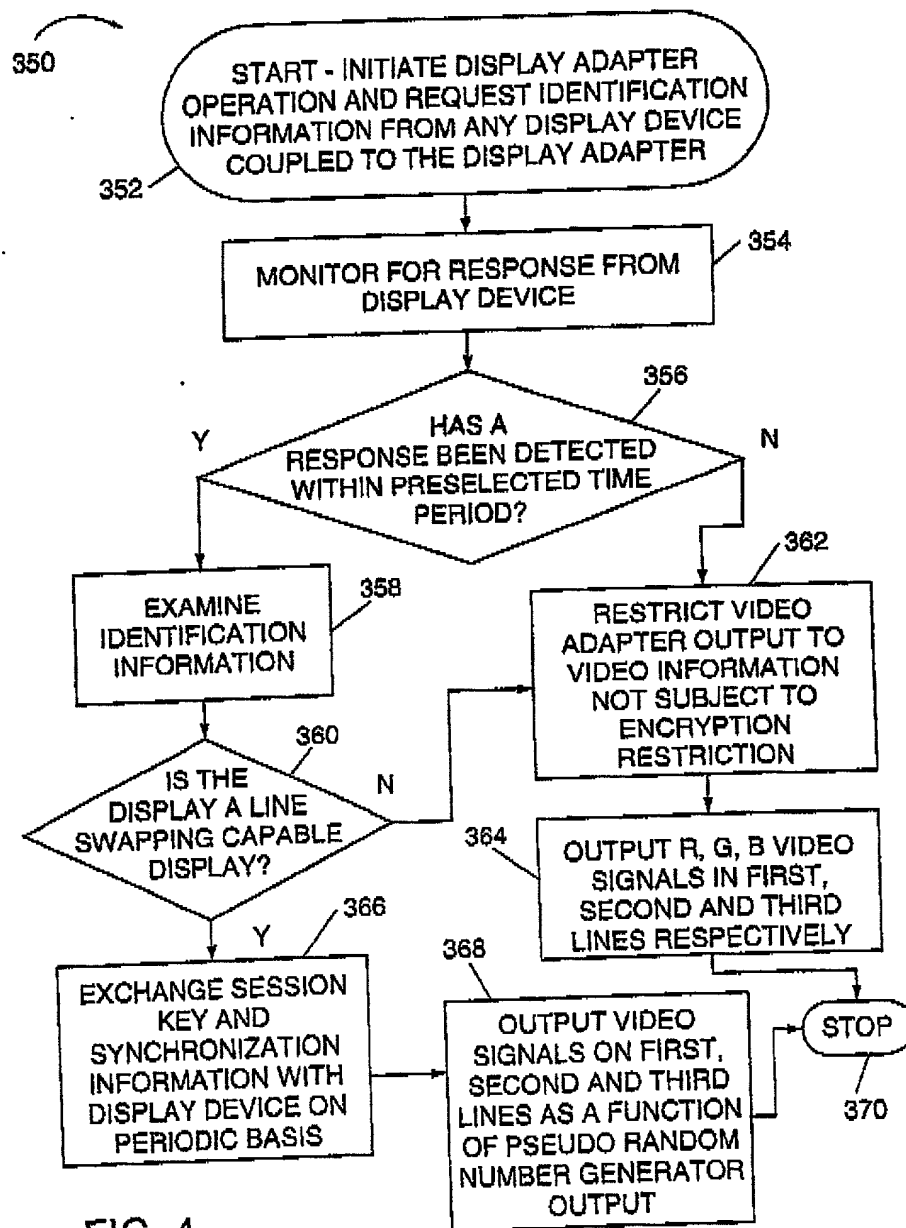


FIG. 4

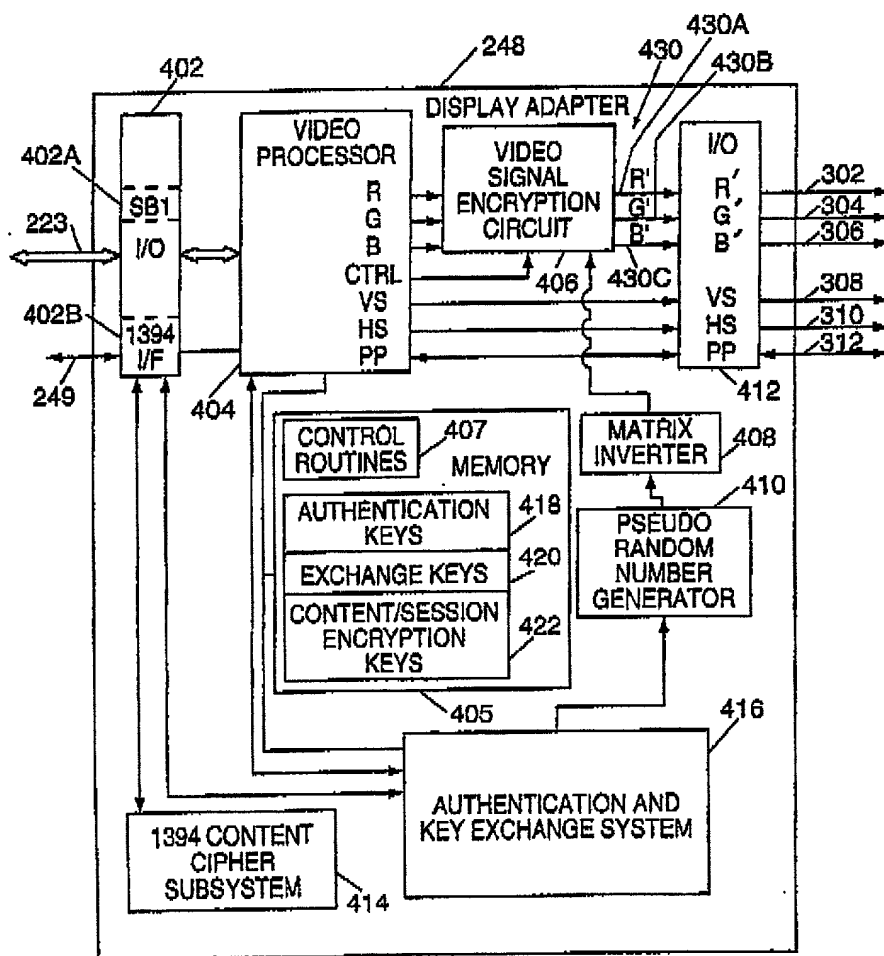


FIG. 5

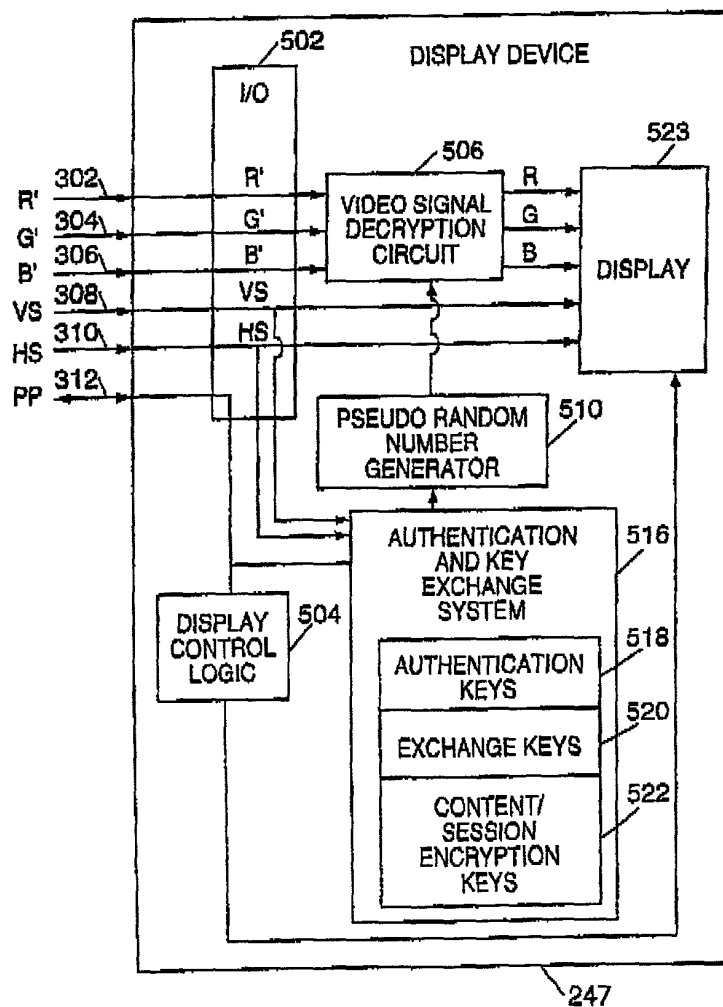


FIG. 6

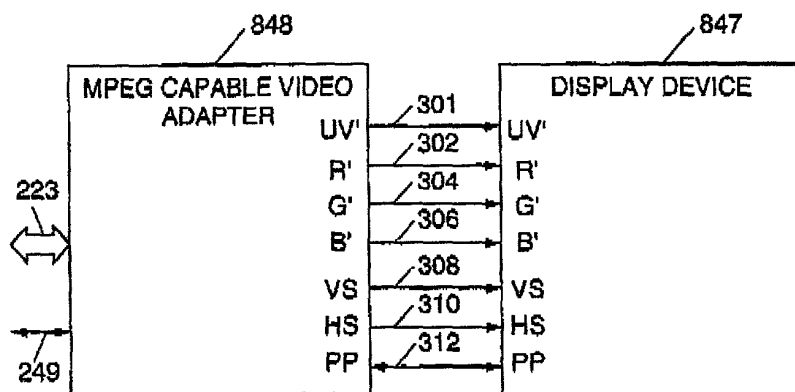


FIG. 8

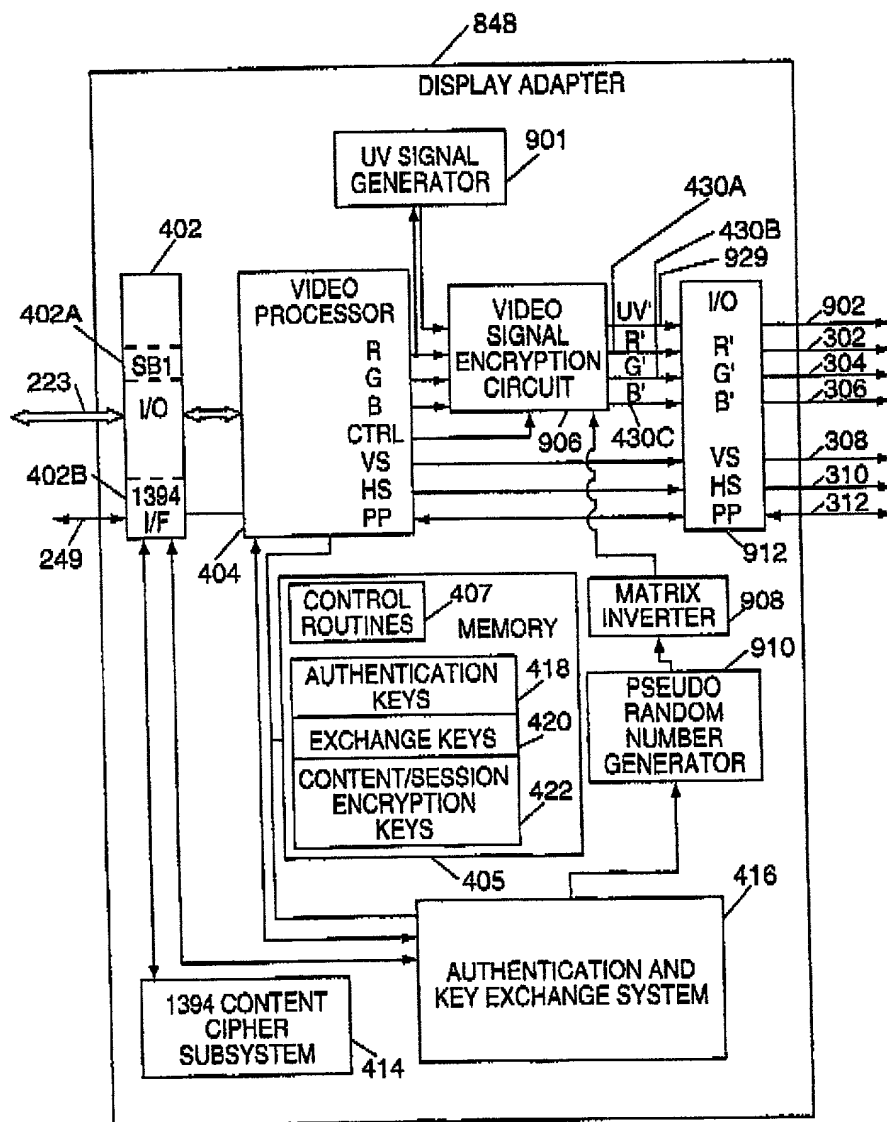


FIG. 9

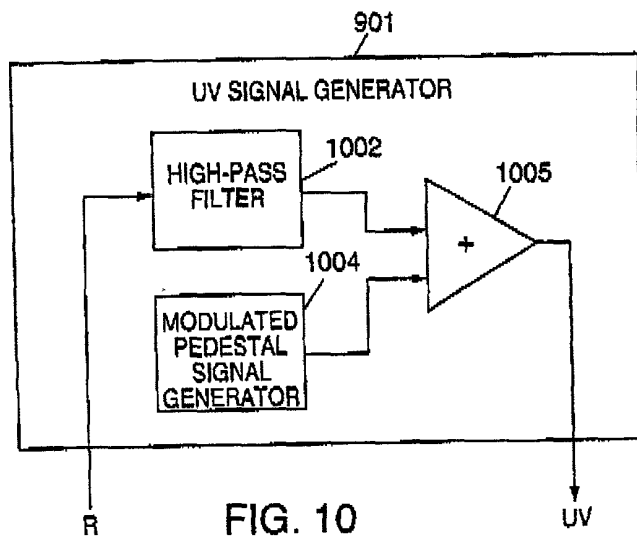


FIG. 10

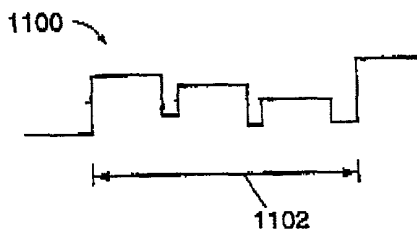


FIG. 11

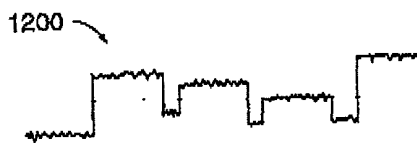


FIG. 12

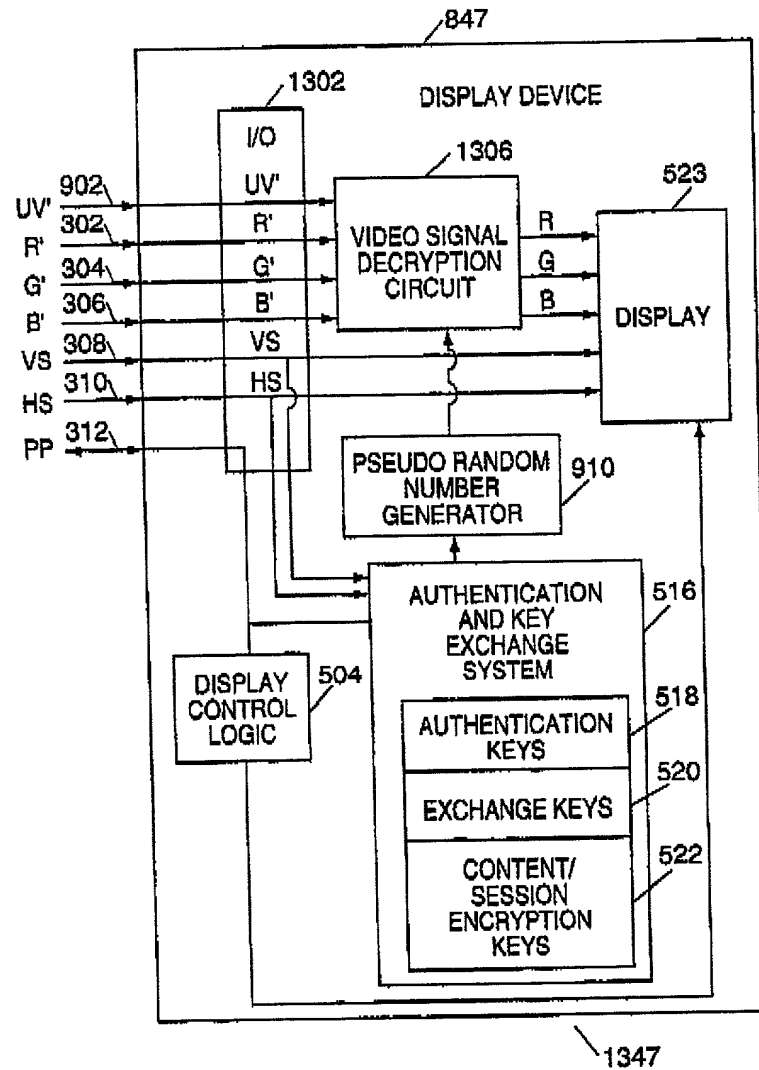


FIG. 13

Country	Year	Population (millions)	Urban population (millions)	Urban population (%)	Population density (per sq km)	Urban population density (per sq km)	Population growth rate (%)	Urban population growth rate (%)	Population growth rate (per 1,000)	Urban population growth rate (per 1,000)
Algeria	1980	10.0	4.0	40.0	100	400	1.5	2.5	15	25
Algeria	1985	10.5	4.5	42.9	105	450	1.8	2.8	18	28
Algeria	1990	11.0	5.0	45.5	110	500	2.0	3.0	20	30
Algeria	1995	11.5	5.5	47.8	115	550	2.2	3.2	22	32
Algeria	2000	12.0	6.0	50.0	120	600	2.4	3.4	24	34
Algeria	2005	12.5	6.5	52.0	125	650	2.6	3.6	26	36
Algeria	2010	13.0	7.0	53.8	130	700	2.8	3.8	28	38
Algeria	2015	13.5	7.5	55.6	135	750	3.0	4.0	30	40
Algeria	2020	14.0	8.0	57.1	140	800	3.2	4.2	32	42
Algeria	2025	14.5	8.5	58.6	145	850	3.4	4.4	34	44
Algeria	2030	15.0	9.0	60.0	150	900	3.6	4.6	36	46
Algeria	2035	15.5	9.5	61.3	155	950	3.8	4.8	38	48
Algeria	2040	16.0	10.0	62.5	160	1000	4.0	5.0	40	50
Algeria	2045	16.5	10.5	63.6	165	1050	4.2	5.2	42	52
Algeria	2050	17.0	11.0	64.7	170	1100	4.4	5.4	44	54
Algeria	2055	17.5	11.5	65.7	175	1150	4.6	5.6	46	56
Algeria	2060	18.0	12.0	66.7	180	1200	4.8	5.8	48	58
Algeria	2065	18.5	12.5	67.6	185	1250	5.0	6.0	50	60
Algeria	2070	19.0	13.0	68.4	190	1300	5.2	6.2	52	62
Algeria	2075	19.5	13.5	69.2	195	1350	5.4	6.4	54	64
Algeria	2080	20.0	14.0	70.0	200	1400	5.6	6.6	56	66
Algeria	2085	20.5	14.5	70.7	205	1450	5.8	6.8	58	68
Algeria	2090	21.0	15.0	71.4	210	1500	6.0	7.0	60	70
Algeria	2095	21.5	15.5	72.1	215	1550	6.2	7.2	62	72
Algeria	2100	22.0	16.0	72.7	220	1600	6.4	7.4	64	74
Algeria	2105	22.5	16.5	73.3	225	1650	6.6	7.6	66	76
Algeria	2110	23.0	17.0	73.9	230	1700	6.8	7.8	68	78
Algeria	2115	23.5	17.5	74.5	235	1750	7.0	8.0	70	80
Algeria	2120	24.0	18.0	75.0	240	1800	7.2	8.2	72	82
Algeria	2125	24.5	18.5	75.5	245	1850	7.4	8.4	74	84
Algeria	2130	25.0	19.0	76.0	250	1900	7.6	8.6	76	86
Algeria	2135	25.5	19.5	76.5	255	1950	7.8	8.8	78	88
Algeria	2140	26.0	20.0	76.9	260	2000	8.0	9.0	80	90
Algeria	2145	26.5	20.5	77.3	265	2050	8.2	9.2	82	92
Algeria	2150	27.0	21.0	77.8	270	2100	8.4	9.4	84	94
Algeria	2155	27.5	21.5	78.2	275	2150	8.6	9.6	86	96
Algeria	2160	28.0	22.0	78.6						

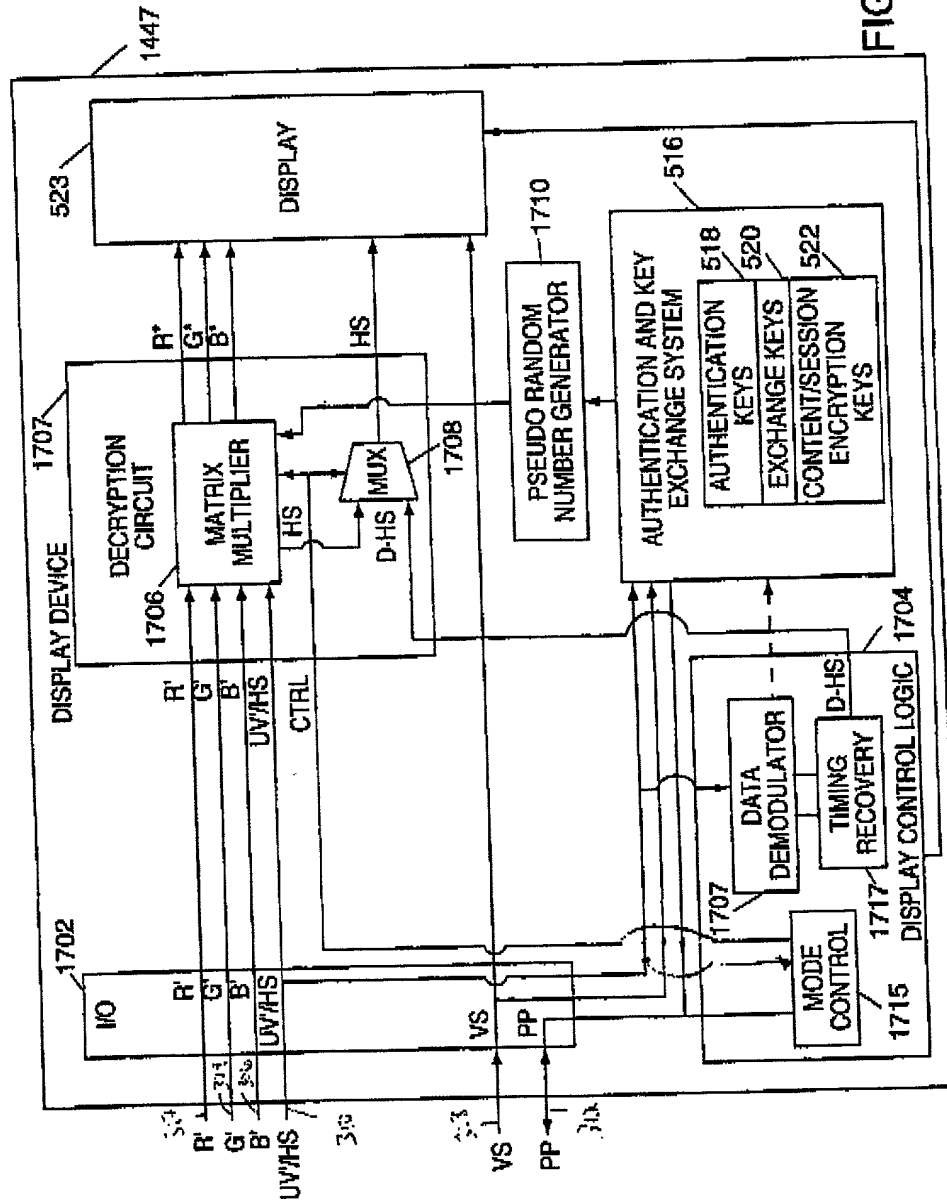


FIG. 17

**DECLARATION AND
POWER OF ATTORNEY
(Utility Patent Application)**

As a below named inventor, I hereby declare:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below), of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**METHODS AND APPARATUS FOR PROTECTING SIGNALS TRANSMITTED BETWEEN
A SOURCE AND DESTINATION DEVICE OVER MULTIPLE SIGNAL LINES**

the specification of which:

- ☒ is attached hereto
- ☐ was filed on _____ as Application Serial
No. _____ with amendment(s) filed _____
- ☐ was filed as PCT international application:
serial number _____ on _____
and was amended under PCT Article 19 on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations section 1.56.

I hereby claim foreign priority benefits under Section 119 of Title 35, United States Code for the above-identified US patent application based on the patent or inventor's certificate identified below and having a filing date before that of the US patent application for which priority is claimed:

Application No. Country Filing Date Priority Claimed
under 35 U.S.C. §119

I hereby claim the benefit under Section 120 and/or
Section 119(e) of Title 35 of the United States Code of any
United States application(s) listed below and, insofar as the
subject matter of each of the claims of this application is not
disclosed in the prior United States application in the manner
provided by Section 112 of Title 35 of the United States Code, I
acknowledge the duty to disclose material information, as
defined in Section 1.56 of Title 37 of the Code of Federal
Regulations, which occurred between the filing date of the prior
application and the national or PCT international filing date of
this application:

Application Serial No.	Filing Date	Status		
		Patented	Pending	Abandoned
Prov. App. S.N. 60/160,603	Oct. 20, 1999		X	

Power of attorney:

As a named inventor, I hereby appoint:

John C. Pokotylo (Reg. No. 36,242)
Michael P. Straub (Reg. No. 36,941)
Daniel D. Crouse (Reg. No. 32,022)
Katie E. Sako (Reg. No. 32,628)

as my attorneys to prosecute this application and to transact
all business in the United States Patent and Trademark Office in
connection therewith.

Direct all correspondence to Customer Number IDON601137 at the
following address:


STRAUB & POKOTYLO
1 Bethany Road
Suite 56, Building 4
Hazlet, New Jersey 07730.

Direct all telephone calls to: (732) 335-1222.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.


First inventor:

Full name: England Paul
last first middle
Residence address: 16659 Northrup Way
street
Bellevue, WA 98008 USA
city, state, zip code country
Post Office address: same as residence
post office & box number

city, state, zip code country
Citizenship: United Kingdom
country
Signature: 
Date: 6/29/00

Second inventor:

Full name: Rosen Andrew D.
last first middle
Residence address: 17031 NE 195th St.
street
Woodinville, WA 98072 USA
city, state, zip code country
Post Office address: same as residence
post office & box number

city, state, zip code country
Citizenship: USA
country
Signature: 
Date: 6-29-2000

Third inventor:

Full name: Yacobi Yacov
last first middle
Residence address: 5050 W. Mercer Way
street
Mercer Island, WA 98040 USA
city, state, zip code country
Post Office address: same as residence
post office & box number

city, state, zip code country
Citizenship: USA and Israel
country

Signature: Yacov Yacobi

Date: June 29, 2000

Fourth inventor:

Full name: Yuval Gideon A.
last first middle
Residence address: 7660 81st Pl SE
street
Mercer Island, WA 98040 USA
city, state, zip code country
Post Office address: same as residence
post office & box number

city, state, zip code country
Citizenship: USA and Israel
country

Signature: (G. YUVAL)

Date: 6/2/00